GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE

12 règles essentielles pour sécuriser vos équipements numériques

CGPME

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •



La cybersécurité est un facteur de productivité, de compétitivité et donc de croissance pour les entreprises.

Quelle que soit sa taille, une PME doit prendre conscience qu'elle peut être à tout moment confrontée à la cybercriminalité. Qu'il s'agisse, par exemple, de malveillances visant à la destruction de données ou d'espionnage économique et industriel, les conséquences des attaques informatiques pour les entreprises, et plus particulièrement les TPE, sont généralement désastreuses et peuvent impacter leur pérennité.

Pour la CGPME, chaque entreprise doit aujourd'hui se doter d'une politique de sécurisation des systèmes d'information inhérente à l'usage des nouvelles technologies.

Si les contraintes financières des petites structures restent un frein à la construction d'une cybersécurité optimale, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique.

Pour recenser ces usages, la Confédération, par le biais de sa Commission Economie Numérique, s'est rapprochée de l'ANSSI.

Fruit d'un partenariat constructif, un guide des bonnes pratiques informatiques a été élaboré afin de sensibiliser les PME sur cette problématique tout en leur apportant les moyens opérationnels de préserver leurs systèmes d'information.

A vous désormais, chefs d'entreprises, de devenir les acteurs de votre propre sécurité !

François Asselin
Président CGPME



Qu'il s'agisse de la numérisation des dossiers de la patientèle d'un cabinet médical, des nouvelles possibilités de paiement en ligne, de la multiplication des échanges par courriel, l'usage de l'informatique s'est généralisé dans les TPE/PME. Corollaire de cette formidable évolution, de nouveaux risques ont émergé : vol de données, escroqueries financières, sabotage de sites d'e-commerce. Leurs conséquences peuvent être lourdes : indisponibilités, coût, atteinte à l'image de l'entreprise et perte de clientèle.

La complexité des menaces, le coût, le manque de personnel et de temps sont souvent autant d'arguments pour justifier un moindre intérêt porté à la sécurité informatique au sein des petites structures. Ces questions sont pourtant essentielles et relèvent souvent de réflexes simples. Il ne faut pas oublier que devoir remédier à un incident dans l'urgence peut s'avérer bien plus coûteux que leur prévention. Les mesures accessibles aux non-spécialistes décrites dans ce guide concourent à une protection globale de l'entreprise, qu'il s'agisse de ses brevets, de sa clientèle, de sa réputation et de sa compétitivité.

La sensibilisation aux enjeux de sécurité informatique de chaque acteur, notamment dans le domaine économique, est au cœur des préoccupations de l'Agence nationale de la sécurité des systèmes d'information. C'est donc tout naturellement que l'ANSSI a souhaité s'associer avec la CGPME (Confédération générale du patronat des petites et moyennes entreprises) pour apporter une expertise qui coïncide avec la réalité rencontrée par les petites structures, dont je n'oublie pas qu'elles constituent 90 % des entreprises françaises. Ce partenariat fructueux nous permet de vous présenter aujourd'hui ce « Guide des bonnes pratiques informatiques » à destination des PME.

Les douze recommandations pratiques qu'il présente sont issues de l'observation directe d'attaques réussies et de leurs causes. Dirigeants et entrepreneurs, n'hésitez pas à vous les approprier pour les mettre en œuvre au sein de vos structures.

Vous souhaitant bonne lecture,

Guillaume Poupard
Directeur général – Agence nationale de la sécurité des systèmes d'information

TABLE DES MATIERES

Pourquoi sécuriser son informatique ?

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages. Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les entreprises. Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours...) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable. La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau...). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise. Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre dans l'entreprise. À cet effet, la sensibilisation des collaborateurs de l'entreprise aux règles d'hygiène informatique est fondamentale et surtout très efficace pour limiter une grande partie des risques.

Réalisé par le biais d'un partenariat entre l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et la CGPME, ce guide a pour objectif de vous informer sur les risques et les moyens de vous en prémunir en acquérant des réflexes simples pour sécuriser votre usage de l'informatique. Chaque règle ou « bonne pratique » est accompagnée d'un exemple inspiré de faits réels auxquels l'ANSSI a été confrontée.

*Les mots en italique marqués d'un * sont expliqués dans le glossaire situé à la fin de ce guide.*

1

Choisir avec soin ses mots de passe

Dans le cadre de ses fonctions de comptable, Julien va régulièrement consulter l'état des comptes de son entreprise sur le site Internet mis à disposition par l'établissement bancaire. Par simplicité, il a choisi un mot de passe faible : 123456. Ce mot de passe a très facilement été reconstitué lors d'une attaque utilisant un outil automatisé : l'entreprise s'est fait voler 10 000 euros.

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance…) et ne figurant pas dans le dictionnaire.

Deux méthodes simples peuvent vous aider à définir vos mots de passe :

- La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;
- La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » : aE2lP,lJ2Géa!

Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle…) ne doivent jamais être réutilisés pour d'autres services.

Il est préférable de ne pas recourir aux outils de stockage de mots de passe. A défaut, il faut s'en tenir à une solution ayant reçu une certification de premier niveau (CSPN)

En entreprise :

- déterminez des règles de choix et de dimensionnement (longueur) des mots de passe et faites les respecter ;
- modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box…) ;
- rappelez aux collaborateurs de ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;
- sensibilisez les collaborateurs au fait qu'ils ne doivent pas préenregistrer leurs mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements…).

2

Mettre à jour régulièrement vos logiciels

Carole, administrateur du système d'information d'une PME, ne met pas toujours à jour ses logiciels. Elle a ouvert par mégarde une pièce jointe piégée. Suite à cette erreur, des attaquants ont pu utiliser une vulnérabilité logicielle et ont pénétré son ordinateur pour espionner les activités de l'entreprise.*

Dans chaque système d'exploitation* (Android, IOS, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs* des mises à jour* de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

Il convient donc, au sein de l'entreprise, de mettre en place certaines règles :

- définissez et faites appliquer une politique de mises à jour régulières :
  - » S'il existe un service informatique au sein de l'entreprise, il est chargé de la mise à jour du système d'exploitation et des logiciels ;
  - » S'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du chef d'entreprise.
- configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles ;
- utilisez exclusivement les sites Internet officiels des éditeurs.

3

Bien connaître ses utilisateurs et ses prestataires

Noémie naviguait sur Internet depuis un compte administrateur de son entreprise. Elle a cliqué par inadvertance sur un lien conçu spécifiquement pour l'attirer vers une page web infectée. Un programme malveillant s'est alors installé automatiquement sur sa machine. L'attaquant a pu désactiver l'antivirus de l'ordinateur et avoir accès à l'ensemble des données de son service, y compris à la base de données de sa clientèle.*

Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur »* et les droits dits « d'administrateur »*.

- Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels de bureautique, de jeu,...), prenez un compte utilisateur. Il répondra parfaitement à vos besoins.
- Le compte administrateur n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels,...).

Les systèmes d'exploitation récents vous permettent d'intervenir facilement sur le fonctionnement global de votre machine sans changer de compte : si vous utilisez un compte utilisateur, le mot de passe administrateur est demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur.

Au sein de l'entreprise :

- réservez l'utilisation au service informatique, si celui-ci existe ;
- dans le cas contraire, protégez-en l'accès, n'ouvrez pour les employés que des comptes utilisateur, n'utilisez pas le compte administrateur pour de la navigation sur Internet ;
- identifiez précisément les différents utilisateurs du système et les privilèges qui leur sont accordés. Tous ne peuvent pas bénéficier de droits d'administrateur ;
- supprimez les comptes anonymes et génériques (stagiaire, contact, presse, etc.). Chaque utilisateur doit être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur ;
- encadrez par des procédures déterminées les arrivées et les départs de personnel pour vous assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et surtout qu'ils sont révoqués lors du départ de la personne.

4

Effectuer des sauvegardes régulières

Patrick, commerçant, a perdu la totalité de son fichier client suite à une panne d'ordinateur. Il n'avait pas effectué de copie de sauvegarde.

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un CD ou un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports.

Avant d'effectuer des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud » ou « informatique en nuage »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques :

   » risques pour la confidentialité des données,
   » risques juridiques liés à l'incertitude sur la localisation des données,
   » risques pour la disponibilité et l'intégrité des données,
   » risques liés à l'irréversibilité des contrats.

- soyez vigilant en prenant connaissance des conditions générales d'utilisation de ces services. Les contrats proposés dans le cadre des offres génériques ne couvrent généralement pas ces risques ;
- autant que possible, n'hésitez pas à recourir à des spécialistes techniques et juridiques pour la rédaction des contrats personnalisés et appropriés aux enjeux de votre entreprise ;
- veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement* avant de les copier dans le « cloud ».

Pour en savoir plus, consultez le guide sur l'externalisation et la sécurité des systèmes d'information réalisé par l'ANSSI.

5

Sécuriser l'accès Wi-Fi de votre entreprise

La borne d'accès à Internet (box) de la boutique de Julie est configurée pour utiliser le chiffrement WEP. Sans que Julie ne s'en aperçoive, un voisin a réussi en moins de deux minutes, à l'aide d'un logiciel, à déchiffrer la clé de connexion. Il a utilisé ce point d'accès Wi-Fi pour participer à une attaque contre un site Internet gouvernemental. Désormais, Julie est mise en cause dans l'enquête de police.*

L'utilisation du Wi-Fi est une pratique attractive. Il ne faut cependant pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes malintentionnées. Pour cette raison l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise : une installation filaire reste plus sécurisée et plus performante.

Le Wi-Fi peut parfois être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre borne d'accès à Internet. Pour ce faire :

- n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès*.Les fournisseurs d'accès à Internet vous guident dans cette configuration en vous proposant différentes étapes, durant lesquelles vous appliquerez ces recommandations de sécurité:
  - » au moment de la première connexion de votre ordinateur en Wi-Fi, ouvrez votre navigateur Internet pour configurer votre borne d'accès. L'interface de configuration s'affiche dès l'ouverture du navigateur. Dans cette interface, modifiez l'identifiant de connexion et le mot de passe par défaut qui vous ont été donnés par votre fournisseur d'accès;
  - » dans cette même interface de configuration, que vous pouvez retrouver en tapant l'adresse indiquée par votre fournisseur d'accès, vérifiez que votre borne dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes) ;
  - » modifiez la clé de connexion par défaut (qui est souvent affichée sur l'étiquette de votre borne d'accès à Internet) par une clé (mot de passe) de plus de 12 caractères de types différents (cf. : 1-Choisissez des mots de passe robustes) ;
  - » ne divulguez votre clé de connexion qu'à des tiers de confiance et changez la régulièrement ;
  - » activez la fonction pare-feu de votre box ;
  - » désactivez votre borne d'accès lorsqu'elle n'est pas utilisée.

- n'utilisez pas les Wi-Fi « publics » (réseaux offerts dans les gares, les aéroports ou les hôtels) pour des raisons de sécurité et de confidentialité ;
- assurez-vous que votre ordinateur est bien protégé par un antivirus et un pare-feu. (Voir aussi Fiche 7 : Protéger ses données lors d'un déplacement). Si le recours à un service de ce type est la seule solution disponible (lors d'un déplacement, par exemple), il faut s'abstenir d'y faire transiter toute donnée personnelle ou confidentielle (en particulier messages, transactions financières). Enfin, il n'est pas recommandé de laisser vos clients, fournisseurs ou autres tiers se connecter sur votre réseau (Wi-Fi ou filaire).
- préférez avoir recours à une borne d'accès dédiée si vous devez absolument fournir un accès tiers. Ne partagez pas votre connexion.

6

Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur

Arthur possède un ordiphone qu'il utilise à titre personnel comme professionnel. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, l'éditeur de l'application peut accéder à tous les SMS présents sur son téléphone.

Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd’hui très peu sécurisés. Il est donc indispensable d’appliquer certaines règles élémentaires de sécurité informatique :

- n’installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l’accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer ;
- en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l’accès à votre terminal et le configurer pour qu’il se verrouille automatiquement ;
- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;
- ne préenregistrez pas vos mots de passe (plus d’informations en fiche 1).

7

Protéger ses données lors de ses déplacements

Dans un aéroport, Charles sympathise avec un voyageur prétendant avoir des connaissances en commun. Lorsque celui-ci lui demande s'il peut utiliser son ordinateur pour recharger son ordiphone, Charles ne se méfie pas. L'inconnu en a profité pour exfiltrer les données concernant la mission professionnelle très confidentielle de Charles.

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation. Il convient de se référer au passeport de conseils aux voyageurs édité par l'ANSSI.

Avant de partir en mission

- n'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires ;
- sauvegardez ces données, pour les retrouver en cas de perte ;
- si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur ;
- apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport ;
- vérifiez que vos mots de passe ne sont pas préenregistrés.

Pendant la mission

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;
- désactivez les fonctions Wi-Fi et Bluetooth de vos appareils ;
- retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone ;

- informez votre entreprise en cas d’inspection ou de saisie de votre matériel par des autorités étrangères ;
- n’utilisez pas les équipements que l’on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance ;
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d’échanger des documents lors d’une présentation commerciale, utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données avec un logiciel d’effacement sécurisé ;
- refusez la connexion d’équipements appartenant à des tiers à vos propres équipements (ordiphone, clé USB, baladeur…)

Après la mission

- effacez l’historique des appels et de navigation ;
- changez les mots de passe que vous avez utilisés pendant le voyage ;
- faites analyser vos équipements après la mission, si vous le pouvez.
- n’utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements (salons, réunions, voyages…) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

8

Être prudent lors de l'utilisation de sa messagerie

Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Jean-Louis a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Jean-Louis le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts;
- si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence;
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing »* ;
- n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

9

Télécharger ses programmes sur les sites officiels des éditeurs

Emma, voulant se protéger des logiciels espions (spyware), a téléchargé un logiciel spécialisé proposé par son moteur de recherche. Sans le savoir, elle a installé un cheval de Troie.*

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie*. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Dans ce contexte, afin de veiller à la sécurité de votre machine et de vos données :

- téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
- pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens ;
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

10

Être vigilant lors d'un paiement sur Internet

Céline a acheté sur Internet des fournitures de bureau pour son entreprise sans vérifier l'état de sécurité du site de commerce en ligne. Ce dernier n'était pas sécurisé. Des attaquants ont intercepté le numéro de carte bancaire de l'entreprise et ont soutiré 1 000 euros.

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordiphone (smartphone), vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet ;
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

Si possible, lors d'un achat en ligne :

- privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire ;
- n'hésitez pas à vous rapprocher votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

11

Séparer les usages personnels des usages professionnels

Paul rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels.

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette, etc.) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle pose des problèmes en matière de sécurité des données (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
- n'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
- de la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.

Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

12

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Alain reçoit un courriel lui proposant de participer à un concours pour gagner un ordinateur portable. Pour ce faire, il doit transmettre son adresse électronique. Finalement, Alain n'a pas gagné mais reçoit désormais de nombreux courriels non désirés.

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.

Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir :
  - ne transmettez que les informations strictement nécessaires ;
  - pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données ;
- ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ;
- pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité (Cf. Guide de la CNIL sur la sécurité des données personnelles) ;
- enfin, utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…).

En résumé ...

Afin de renforcer efficacement la sécurité de vos équipements communicants et de vos données, vous pouvez compléter les douze bonnes pratiques de ce guide par les mesures suivantes :

- désignez un correspondant/référent pour la sécurité informatique dans les entreprises ;
- rédigez une charte informatique ;
- chiffrez vos données et vos échanges d'information à l'aide de logiciels de chiffrement* ;
- durcissez la configuration de votre poste et utilisez des solutions de sécurité éprouvées (pare-feux*, antivirus*) ;
- avant d'enregistrer des fichiers provenant de supports USB sur votre ordinateur, faites-les analyser par un antivirus ;
- désactivez l'exécution automatique des supports amovibles depuis votre ordinateur ;
- éteignez votre ordinateur pendant les périodes d'inactivité prolongée (nuit, week-end, vacances,...) ;
- surveillez et monitorez votre système, notamment en utilisant les journaux d'événements, pour réagir aux événements suspects (connexion d'un utilisateur hors de ses horaires habituels, transfert massif de données vers l'extérieur de l'entreprise, tentatives de connexion sur un compte non actif,...).

Pour aller plus loin

- **ANSSI** : http://www.ssi.gouv.fr
- **CNIL** : http://www.cnil.fr
- **Délégation à l'intelligence économique (D2IE)** : http://www.intelligence-economique.gouv.fr
- **Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Police nationale)** : http://www.internet-signalement.fr

En cas d'incident

Vous n'avez pas eu le temps de mettre en œuvre les règles décrites dans ce guide ou les attaquants ont réussi à les contourner. Ne cédez pas à la panique, et ayez les bons réflexes.

- en cas de comportement inhabituel de votre ordinateur, vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation,...) ;
- déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez-là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque ;
- prévenez votre hiérarchie, ainsi que le responsable de la sécurité, au téléphone ou de vive voix, car l'intrus peut-être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque ;
- faites faire une copie physique du disque ;
- faites rechercher les traces disponibles liées à la compromission. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.) ;
- déposez une plainte auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société, de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris et petite couronne), ou de la Direction générale de la sécurité intérieure. Retrouvez plus d'informations sur le site de l'ANSSI : *www.ssi.gouv.fr/en-cas-dincident/* ;
- après l'incident : réinstallez complètement le système d'exploitation à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information.

Glossaire

- **antivirus :** logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants ;
- **cheval de Troie :** programme qui s'installe de façon frauduleuse pour remplir une tâche hostile à l'insu de l'utilisateur (espionnage, envoi massif de spams,...) ;
- **chiffrement :** procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement ;
- **compte d'administrateur :** compte permettant d'effectuer des modifications affectant les utilisateurs (modification des paramètres de sécurité, installer des logiciels...) ;
- **logiciel espion :** logiciel malveillant qui s'installe dans un ordinateur afin de collecter et transférer des données et des informations, souvent à l'insu de l'utilisateur.
- **Fournisseur d'Accès Internet (FAI) :** organisme (entreprise ou association) offrant une connexion à Internet ;
- **mise à jour :** action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel ;
- **pare-feu (firewall) :** logiciel et/ou matériel permettant de protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet, protection d'un réseau d'entreprise,...) en filtrant les entrées et en contrôlant les sorties selon les règles définies par son utilisateur ;
- **paquet :** unité de transmission utilisée pour communiquer ;
- **phishing (hameçonnage) :** méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.
- **routeur :** élément intermédiaire dans un réseau informatique assurant la distribution des paquets de données en déterminant le prochain nœud de réseau auquel un paquet doit être envoyé ;
- **système d'exploitation :** logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels ;

- **utilisateur :** personne qui utilise un système informatique ;
- **WEP :** protocole de sécurité permettant de fournir aux utilisateurs de réseaux locaux sans fil une protection contre le piratage ;
- **Wi Fi :** connexion Internet sans fil
- **WPA 2 :** standard de sécurité protégeant les utilisateurs contre le piratage des réseaux sans fil devant se substituer au système WEP jugé insuffisant.

Contacts

CGPME

Amélie JUGAN

ajugan@cgpme.fr

ANSSI

communication@ssi.gouv.fr

Guide téléchargeable sur les sites :

www.cgpme.fr

www.ssi.gouv.fr

Version 1.1 - Mars 2015
20150326-1517

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
www.ssi.gouv.fr / communication@ssi.gouv.fr